ARMY RESEARCH LABORATORY

# Piecewise Linear Noise Modulation (PLNM)

by Lisa M. Marvel, Malcolm S. Taylor,
and Charles G. Boncelet, Jr.

ARL-TR-2450

April 2001

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

**Army Research Laboratory**
Aberdeen Proving Ground, MD 21005-5067

**ARL-TR-2450** **April 2001**

# Piecewise Linear Noise Modulation (PLNM)

Lisa M. Marvel, Malcolm S. Taylor, and Charles G. Boncelet, Jr.
Computational and Information Sciences Directorate, ARL

# Abstract

We present a modulation technique to embed a binary bitstream within a real-valued Gaussian noise sequence. The modulation produces a sequence which possesses an optimal minimum distance property that promotes accurate detection when the sequence has been exposed to noise. Because the modulated sequence possesses Gaussian properties and has low power, it is difficult for unintended parties to intercept and detect the signal. The technique can be used to hide information in a signal that is then added to a carrier for a variety of applications.

# Table of Contents

INTENTIONALLY LEFT BLANK.

# List of Figures

INTENTIONALLY LEFT BLANK.

# 1. Introduction

In many applications, the capability to conceal the transmission of information is desired. Such is the case for applications of steganography, watermarking, and tamperproofing. An effective method of concealing information is to exploit the properties of existing systems; there are numerous techniques currently in existence [1, 2, 3].

For example, various types of noise exist in the output of many electronic systems, natural digital images, and audio signals. We can take advantage of this phenomenon by concealing or embedding information in a noise signal. This signal can then be added to or used as a replacement for the inherent noise in the system. If this embedded signal maintains the characteristics of the inherent noise, it will be difficult, if not impossible, to distinguish the signal from the carrier's innate noise.

From Shannon's information theory, we know that in the presence of interference and jamming, a communicator's best waveform should statistically appear as Gaussian noise [4, 5]. This is true because maximum entropy is obtained from Gaussian statistics due to the wideband spectral properties of the waveform.

We apply Shannon's recommendation during the development of the Piecewise Linear Noise Modulation (PLNM) scheme by requiring that the modulated output produce a sequence that appears as Gaussian noise, regardless of the value of the data signal. This Gaussian noise signal may then be added to a carrier of some type to transmit the embedded information. Furthermore, because interference caused by the transmission channel or imperfect carrier recovery may lead to problematic detection of the embedded data signal, a minimum Euclidean distance property among the modulated values is desired.

PLNM embeds binary information within a real-valued Gaussian noise sequence. The PLNM output maintains a minimum Euclidean distance, proportional to the power of the embedded signal, to allay the effects of distortion on the demodulated signal. The carrier requirements for our system are very flexible. In general, the embedded waveform can be added to any signal that is typically exposed to noise that is modelled as white Gaussian noise. The PLNM technique yields good performance and was employed in the steganographic system presented by Marvel et al. [2].

In the following section, we present background and motivation for our noise modulation technique by citing the parallels and distinctions between PLNM and traditional spread spectrum communication. We then describe a simple antipodal noise modulation technique and its problematic detection in section 3. Then in section 4, we present the PLNM scheme along with its mathematical foundation. Next we use the information presented thus far to compare the two noise modulation techniques in section 5. Finally, in section 6 we draw conclusions and present directions for future research.

## 2. Background

Although both PLNM and traditional spread spectrum communication techniques have similar communication objectives, there are obvious contrasts between the two. Both methods can be used to generate a signal that has low power, a robustness to interference, and is difficult to detect. The spread spectrum signal is generated by modulating a data signal onto a wideband carrier so that the resultant transmitted signal has a much larger bandwidth than the original bandwidth of the data and is relatively insensitive to the value of the data signal [6]. PLNM operates in a analogous manner by embedding a binary data signal within a wideband Gaussian noise sequence. Both systems are typically capable of operating at low power, thereby providing a signal that is difficult to detect and that possesses the interference immunity of a wideband waveform. Furthermore, PLNM relies on the concept of a stored-reference spread spectrum [7], where an identical key and pseudorandom number generator are necessary at the transmitter and receiver.

In a traditional spread spectrum system, the wideband signal is obtained by modulating the data signal with a spread spectrum code generator and then an RF oscillator via frequency or phase modulation. In contrast, PLNM is an amplitude modulation scheme that generates a real-valued noise sequence that can replace or be added to inherent noise in a system. The selection of this system is arbitrary; for example, a digital image or audio sequence can function as a carrier. Detection issues related to signal recovery in spread spectrum are addressed by adding redundancy with the binary spread spectrum code and applying carrier recovery techniques. PLNM provides improved detection performance by providing a minimum distance property that is proportional to the noise signal power. Additional error protection may be obtained by encoding the data signal via an error control code whose rate depends on anticipated carrier recovery performance and channel noise. Furthermore, since the PLNM noise signal is added to the carrier (typically an image or audio sequence), carrier acquisition may be performed using a variety of noise removal filters. The challenge of synchronization is trival because it is addressed by the synchronization of the carrier of its format (e.g., image, audio, video, etc.).

## 3. Simple Antipodal Noise Modulation

Let us begin by describing an antipodal noise modulation technique, similar to the one used by Hartung and Girod [3]. Assume that the message signal $m$ is a bilevel signal consisting of symbols from $\{-1, +1\}$, and the noise sequence $n \in \Re$ is generated by a pseudorandom number generator emulating a Gaussian distribution with zero mean and variance, $\sigma^2$ *. The value of $\sigma^2$ can be adjusted to provide a desired amount of robustness, but is limited by the susceptibility of detection (in the sense of low probability of detection).

*In what follows, we will adopt the notation $N(\mu, \sigma^2)$ to represent the Gaussian distribution with mean $\mu$ and variance $\sigma^2$.

The two signals are modulated by simple multiplication,

$$s(n_i, m_i) = n_i * m_i. \tag{1}$$

The modulated signal, $s \in \Re$, is a sequence possessing a Gaussian distribution with zero mean and variance $\sigma^2$. The signs of the message bit and the noise sequence determine the sign of the modulated signal. Since the noise sequence is symmetric about zero, a change in sign preserves the Gaussian distribution of the signal [8].

The demodulation process is straightforward. The sequence $n$ is replicated at the receiver, and the sign of each symbol of this sequence is compared to the sign of the corresponding symbol in the received modulated sequence, $\hat{s}$, to recover an estimated value of the message sequence, $\hat{m}$, as follows:

$$\hat{m}_i = \text{sign}\left(\frac{\hat{s}_i}{n_i}\right). \tag{2}$$

Even though this modulation method meets the necessary requirements of producing a Gaussian sequence, regardless of the distribution of the message sequence, a major deficiency lies with detecting this signal. Because the modulated signal must follow a Gaussian distribution, most of the sample values occur in the vicinity of zero, with fewer values in the tails. Moreover, only the variation of the sign of the received signal indicates the value of the encoded message bits. Although the distance between the values of the modulated signal for both values of m,

$$D = |s(n_i, m_i = -1) - s(n_i, m_i = +1)| = 2|n_i|, \tag{3}$$

is large for extreme values of the waveform, it is much more often small, in accordance with the Gaussian distribution.

In most instances, when the modulated signal is exposed to external noise from the effects of the carrier or the transmission channel, correct detection of the encoded message sequence is problematic. As with many communication signals that may be exposed to noise, we want the points within our signal constellation as far apart as possible, reflecting a large minimum distance.

This minimum distance is defined as the smallest Euclidean distance between all pairs of distinct points in the signal constellation,

$$d_{min} = \min_i |s(n_i, m_i = -1) - s(n_i, m_i = +1)| \equiv \min_i 2|n_i| = 2 \min_i |n_i|. \tag{4}$$

Communication constellations are typically compared by their $d_{min}$. If the modulated signal incurs noise or distortion, the larger the minimum distance, the more distortion the modulated signal can incur and still be demodulated correctly. However, if the distortion is greater than the threshold value $d_{min}/2$, then a demodulation error will occur.

With this simple system, $d_{min} = 0$. To improve detection performance, it is desirable for minimum distance to be as large as possible. This will promote reliable recovery of the estimate of $\hat{s}$.

# 4. Piecewise Linear Noise Modulation (PLNM) Scheme

Under the constraint that the modulated signal maintain a Gaussian distribution, an improved modulation technique should modulate keyed pseudorandom values with the bilevel message bits and produce a sequence of real numbers that follow a Gaussian distribution and yield a large minimum distance.

Formally, if $x_1, x_2, \ldots$ represents a random sequence from a Gaussian distribution, $N(0, \sigma^2)$, we want to determine a transformation $t^*$ such that $t^*(x_1), t^*(x_2), \ldots$ is also distributed $N(0, \sigma^2)$ and satisfies the expression

$$\max_{t \in \Omega} \min_i |x_i - t(x_i)|, \tag{5}$$

where $\Omega$ is the set of all transformations of $N(0, \sigma^2)$ onto itself.

To aid in the delineation of $\Omega$, we will appeal to the relationship between a continuous distribution and the uniform distribution on the unit interval [9]. Simply stated, for any continuous random variable $x$, with distribution $f(x)$ and cumulative distribution function (cdf) $F(x)$, $F(x)$ transforms the variate $x$ into a variate distributed uniformly on the unit interval. Symbolically, $F(x) \sim U(0,1)$, where the notation "$\sim$" denotes "distributed" and $U(0,1)$ the uniform distribution on the unit interval. Conversely, the inverse mapping $F^{-1}(u)$ maps a uniform variate into a variate having distribution $f(x)$.

This means that $\forall\, t \in \Omega$, the transformation $t : N(0, \sigma^2) \rightarrow N(0, \sigma^2)$ can be expressed as

$$t(x) = \Phi^{-1}(g(\Phi(x))), \tag{6}$$

where $\Phi(\cdot)$ denotes the Gaussian cdf, and the function $g(\cdot)$ is a mapping of the unit interval onto itself. Expressing $t(x)$ as a composite function facilitates our inquiry since (i) it establishes that $\forall\, t \in \Omega\ \exists$ a unique bijection $g$ of the unit interval, and it emphasizes that (ii) the bijection $g$ must also be distribution preserving. It is therefore sufficient to limit our search for $t^*$ to consideration of the set of all mappings of $U(0,1)$ onto itself.

Consider the transformation that produces the modulation points for the antipodal modulation method presented in Section 3. Let $u_1, u_2, \ldots$ be a random sequence from $U(0,1)$. The transform

$$g(u) = 1 - u \qquad 0 \leq u \leq 1, \tag{7}$$

shown in Figure 1, yields $g(u_1), g(u_2), \ldots$ from which the modulated signal of the antipodal modulation system can be constructed as

$$s(u,m) = \begin{cases} \Phi^{-1}(u) & m = +1 \\ \Phi^{-1}(g(u)) & m = -1. \end{cases} \tag{8}$$

For $u = \frac{1}{2}$, $g(u) = u$, and the distance (3) is zero. In this instance, the message bit $m_i$ cannot be recovered, even in the absence of noise.

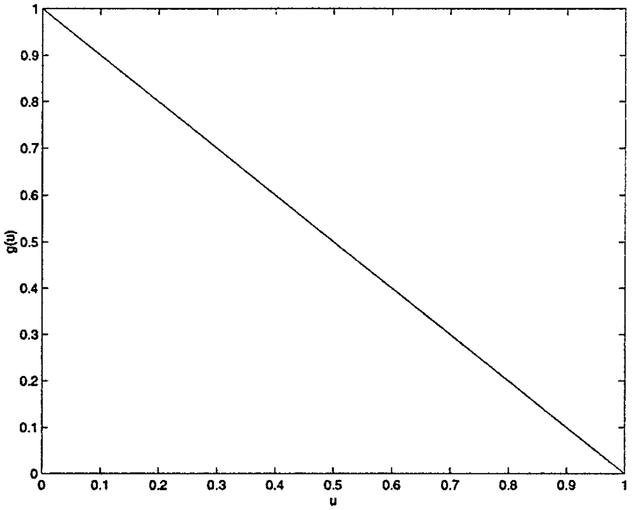

**Figure 1. Transformation for Antipodal Noise Modulation**

Now consider, as the basis for PLNM, the following transformation:

$$g(u) = \begin{cases} u + \frac{1}{2} & 0 \le u \le \frac{1}{2} \\ u - \frac{1}{2} & \frac{1}{2} < u \le 1 \\ 0 & otherwise. \end{cases} \tag{9}$$

As can be seen in Figure 2, $g(u)$ is piecewise linear with a single discontinuity at $u = \frac{1}{2}$.

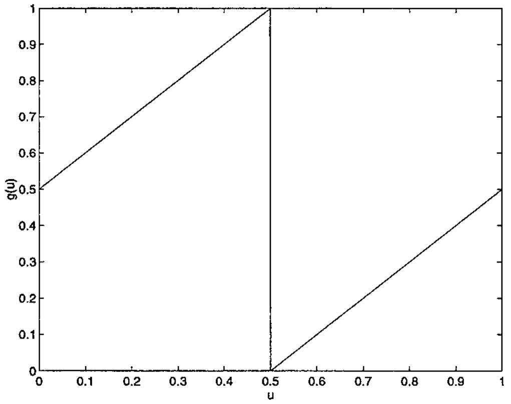

**Figure 2. Transformation for PLNM**

To encode, each element of the modulated signal sequence $s$ is formed by selecting from $u$ or $g(u)$, arbitrated by the elements of the message signal, $m$, and transformed to a Gaussian random value, as prescribed in (8).

Demodulation of the modulated sequence is accomplished by first regenerating both $\Phi^{-1}(u)$ and $\Phi^{-1}(g(u))$ at the receiver and calculating a threshold as the midpoint. The estimated modulated signal is then compared to this threshold to determine the estimated value of the encoded message.

## 4.1 Mathematical Foundation

In this section we focus on relation (9) in the search for a transformation $t^*$ that maximizes the minimum distance between the two possible modulated values as expressed in (5). We first establish that $g(u)$ in (9) preserves the uniform distribution requirement. This condition is necessary to assure that when the inverse Gaussian cdf, $\Phi^{-1}(\cdot)$, is applied, the inverse value will follow a Gaussian distribution. Then we show that the transform (9) is optimal in maximizing the minimum distance between $u$ and $g(u)$. We then proceed to quantify the minimum distance between $\Phi^{-1}(u)$ and $\Phi^{-1}(g(u))$. Finally, we embed $g(u)$ into a more general result characterizing the family of piecewise linear transformations of the type considered here.

### 4.1.1 Distribution of the Transformed Variable

We establish that $g(u) \sim U(0,1)$ by showing that its moment generating function coincides with that of the uniform distribution.

If $f(x)$ is the probability distribution function of a random variable $X$, the moment generating function of $g(X)$ is defined [10] as

$$M_{g(x)}(t) = \int_{-\infty}^{\infty} e^{tg(x)} f(x) dx. \tag{10}$$

Now, let $u \sim U(0,1)$ and let

$$g(u) = \begin{cases} u + \frac{1}{2} & 0 \leq u \leq \frac{1}{2} \\ u - \frac{1}{2} & \frac{1}{2} < u \leq 1 \\ 0 & otherwise. \end{cases} \tag{11}$$

Then, the moment generating function for $g(U)$ is

$$\begin{aligned} M_{g(u)}(t) &= \int_{-\infty}^{\infty} e^{tg(u)} f(u) du \\ &= \int_{0}^{\frac{1}{2}} e^{t(u+\frac{1}{2})} du + \int_{\frac{1}{2}}^{1} e^{t(u-\frac{1}{2})} du & (12) \\ &= \frac{1}{t}(e^t - 1). & (13) \end{aligned}$$

The Uniqueness Theorem [11] asserts the following: Let $X$ and $Y$ be two random variables with moment generating functions $M_X(t)$ and $M_Y(t)$, respectively. If $M_X(t) = M_Y(t)$ for all values of $t$, then $X$ and $Y$ have the same probability distribution.

Since $M_{g(u)}(t) = \frac{1}{t}(e^t - 1) = M_{U(0,1)}(t)$ — the moment generating function for a $U(0,1)$ variate [12] — the result is established.

### 4.1.2 Optimality Condition

Let $\mathcal{F} = \{f_\iota\}_{\iota \in I}$ denote the class of bijections of the unit interval indexed over the set $I$. For the value $x = \frac{1}{2}$, the inequality

$$|x - f(x)| = |\frac{1}{2} - f(\frac{1}{2})| \leq \frac{1}{2} \tag{14}$$

holds $\forall\, f_\iota \in \mathcal{F}$; therefore,

$$\max_{f_\iota \in \mathcal{F}} \min_{x \in [0,1]} |x - f(x)| \leq \frac{1}{2}. \tag{15}$$

Consider the transformation (11). Since

$$|u - g(u)| = \frac{1}{2} \quad \forall\, u \ \in [0,1], \tag{16}$$

we have

$$\min_{u \in [0,1]} |u - g(u)| = \frac{1}{2}; \tag{17}$$

but $g \in \mathcal{F}$, therefore $g(u)$ satisfies condition (15).

This establishes that the piecewise linear function (11) is an optimal transformation on the unit interval, in that the upper bound, $\frac{1}{2}$ in inequality (15), is everywhere assumed.

### 4.1.3 Minimum Euclidean Distance

We begin by expressing the distance between the possible modulation values of our piecewise linear transformation as

$$D = \left|\Phi^{-1}(u) - \Phi^{-1}(g(u))\right|. \tag{18}$$

To find the maximum or minimum of a differentiable function, we would investigate the points at which the derivative is equal to 0. However, the inverse Gaussian cdf, $\Phi^{-1}$, does not exist in closed form, so we are denied a direct approach to determine the minimum value of the distance $D$.

Now consider the signed difference:

$$\Phi^{-1}(u) - \Phi^{-1}(u + \frac{1}{2}), \ \ 0 \leq u < \frac{1}{2}. \tag{19}$$

By definition, the $u$th percentile of a normal variate, $x_u$, satisfies the following relations:

$$\Phi(x_u) = \int_{-\infty}^{x_u} \phi(t)dt = u; \qquad \Phi^{-1}(u) = x_u, \qquad 0 \leq u \leq 1 \tag{20}$$

where $\Phi'(\cdot) = \phi(\cdot)$, the normal distribution function.

On the interval $0 < u < \frac{1}{2}$, we have

$$\Phi^{-1}(u) - \Phi^{-1}(g(u)) = \Phi^{-1}(u) - \Phi^{-1}(u + \frac{1}{2}) = x_u - x_{(u+\frac{1}{2})}. \tag{21}$$

Consider now the subinterval $0 < u < \frac{1}{4}$ and an arbitrarily small $\epsilon > 0$ such that

$$u + \epsilon \in (0, \frac{1}{4}) \text{ and } g(u+\epsilon) = u + \frac{1}{2} + \epsilon \in (\frac{1}{2}, \frac{3}{4}). \tag{22}$$

For every $\epsilon > 0$ satisfying (22) $\exists\ \delta = \delta(u, \epsilon)$ such that

$$\int_a^b \phi(t)dt = \epsilon = \int_c^d \phi(t)dt, \tag{23}$$

where

$$a = x_u \qquad b = x_{(u+\epsilon)} = x_u + \delta_1(u, \epsilon), \tag{24}$$

$$c = x_{(u+\frac{1}{2})} \quad d = x_{(u+\frac{1}{2}+\epsilon)} = x_{(u+\frac{1}{2})} + \delta_2(u, \epsilon). \tag{25}$$

But for $u \in (0, \frac{1}{4})$, the normal distribution function $\phi(x)$ for $x_u \leq x \leq x_u + \delta_1(u, \epsilon)$ is everywhere less than $\phi(x)$ for $x_{(u+\frac{1}{2})} \leq x \leq x_{(u+\frac{1}{2})} + \delta_2(u, \epsilon)$ as illustrated in Figure 3.

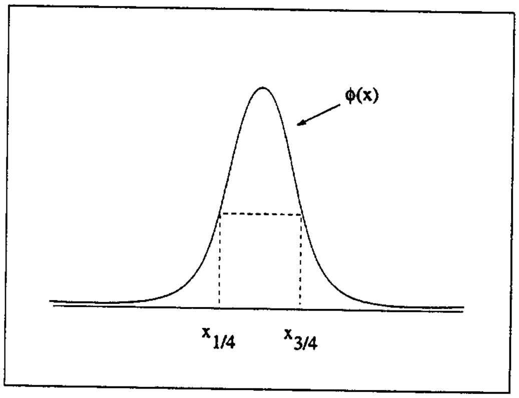

**Figure 3. Distance Between Modulation Points, $u = \frac{1}{4}$**

According to the Mean-Value Theorem [13]: If a function $f(x)$ is continuous on a closed interval $[a, b]$, then there exists a number $x'$, $a \leq x' \leq b$, for which

$$\int_a^b f(x)dx = f(x')(b - a). \tag{26}$$

Application of the Mean Value Theorem to each of the integrals in (23) yields

$$\phi(x')(b - a) = \phi(x'')(d - c). \tag{27}$$

But $0 < \phi(x') < \phi(x'')$; therefore, $b - a > d - c$. Substituting and rearranging the inequality, we obtain

$$x_u - x_{(u+\frac{1}{2})} < x_{(u+\epsilon)} - x_{(u+\frac{1}{2}+\epsilon)}, \tag{28}$$

or alternatively, from (21)

$$\Phi^{-1}(u) - \Phi^{-1}(g(u)) < \Phi^{-1}(u+\epsilon) - \Phi^{-1}(g(u+\epsilon)). \tag{29}$$

However, $u \in (0, \frac{1}{4})$ is arbitrary and $\epsilon > 0$ is arbitrarily small; this assures that $\Phi^{-1}(u) - \Phi^{-1}(g(u))$ — although negative — is strictly monotonically increasing on the interval $(0, \frac{1}{4})$.

The subinterval boundary point, $u = \frac{1}{4}$, requires special attention. For this value of $u$, $g(u) = \frac{3}{4}$ and

$$\Phi^{-1}(u) - \Phi^{-1}(g(u)) = x_{\frac{1}{4}} - x_{\frac{3}{4}}. \tag{30}$$

For the symmetric Gaussian distribution the relation

$$x_\alpha = -x_{1-\alpha}, \quad 0 \leq \alpha \leq 1 \tag{31}$$

holds, and hence

$$\Phi^{-1}(u) - \Phi^{-1}(g(u)) = 2x_{\frac{1}{4}}. \tag{32}$$

Up to now, our assumption has been that $x \sim N(0, \sigma^2)$; to transform to the standard normal variate we evaluate $(x - \mu)/\sigma = z \sim N(0,1)$ to obtain

$$x_{\frac{1}{4}} = \sigma * z_{\frac{1}{4}} = (-0.675)\sigma. \tag{33}$$

A plot of the signed difference is shown in Figure 4 for noise power $\sigma^2 = 1$. An entirely analogous argument to that detailed for the subinterval $(0, \frac{1}{4})$ holds for the remaining subintervals $(\frac{1}{4}, \frac{1}{2})$, $(\frac{1}{2}, \frac{3}{4})$, and $(\frac{3}{4}, 1)$. As can be seen, local minima for the difference $D$ occur at $u = \frac{1}{4}$ and $u = \frac{3}{4}$ where $d_{\min} = 1.35\sigma$.

### 4.1.4 Results for Gaussian Distribution

In this section, we determine the specific properties that an optimal solution $t^*$ in expression (5) must possess.

If $X$ is a continuous random variable with distribution $f_X(x)$, and $Y = g(X)$ is an invertible function of $X$, the well-known result [8]:

$$f_Y(y) = f_X(g^{-1}(y))|\frac{d}{dy}g^{-1}(y)|, \tag{34}$$

provides the distribution of the variable $Y$. In our investigation, $X \sim U(0,1)$ and $Y = g(X)$ is defined in (11).

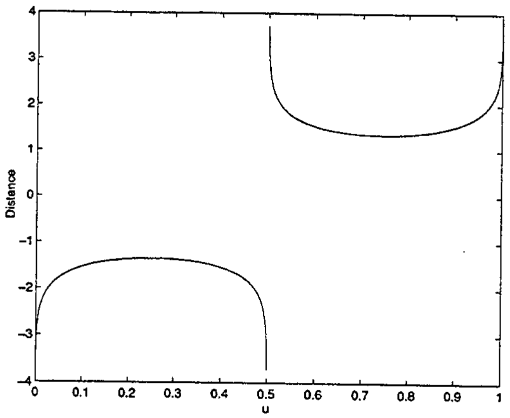

**Figure 4. PLNM Signed Distance, $D$ for $\sigma^2 = 1$**

Consider $f_X(g^{-1}(y))$ in (34); $g^{-1}(y) : [0,1] \rightarrow [0,1]$ is one-to-one and onto. This requires that $f_X(g^{-1}(y)) = 1$ for $0 \leq y \leq 1$. Now consider $\frac{d}{dy}g^{-1}(y)$, where

$$g^{-1}(y) = \begin{cases} y + \frac{1}{2} & 0 \leq y \leq \frac{1}{2} \\ y - \frac{1}{2} & \frac{1}{2} < y \leq 1. \end{cases} \tag{35}$$

The inverse $g^{-1}(y)$ has a discontinuity at $y = \frac{1}{2}$, so the derivative $\frac{d}{dy}g^{-1}(y)$ does not exist at that point; however, $\frac{d}{dy}g^{-1}(y) = 1$ for $0 < y < 1$ and $y \neq \frac{1}{2}$. Therefore, from equation (34), $f_Y(y) = 1$ for $0 < y < 1$ and $y \neq \frac{1}{2}$.

In other words, the random variable $Y$ is distributed uniformly on the unit interval $[0,1]$ except for a set of measure zero (at $y = \frac{1}{2}$). Moreover, any transformation of the uniform random variable $X$, $Y = g(X)$ must be of the form $Y = X + c$, where $c$ is a constant, if the constraint that $Y \sim U(0,1)$ is to be satisfied.

The result that $Y \sim U(0,1)$ was already established in section (4.1.1), where we employed the moment generating function to arrive at the same conclusion. However, at this juncture, we have gone beyond section (4.1.1) in two important respects. The point of discontinuity, $y = \frac{1}{2}$, has been identified as requiring special attention; and, we now know that the transformation $g(\cdot)$ in expression (6) must be of the form $Y = X + c$ when $t(\cdot) = t^*(\cdot)$.

To accommodate the discontinuity at $y = \frac{1}{2}$, it is sufficient to say that $Y \sim U(0,1)$ except on a set of measure zero. The important point in application is that the discontinuity has no impact on the PLNM procedure. As a matter of fact, a finite number of discontinuities will still hold probability measure zero.

### 4.1.5 Unifying Result

What remains to be established is that (9) gives rise to an optimal solution to the fundamental problem expressed in (5)–(6); i.e., we need to show that a solution to:

$$\max_{f \in \mathcal{F}} \min_{u \in [0,1]} |u - g(u)|, \tag{36}$$

is sufficient to assure that

$$\max_{g\in\Omega} \min_{u\in[0,1]} \left|\Phi^{-1}(u) - \Phi^{-1}(g(u))\right| \tag{37}$$

is also satisfied. We will address this problem with the aid of the following theorem.

**Theorem:** Let $g(u)$ be a piecewise linear bijection of the unit interval of the form

$$g(u) = \begin{cases} u+c & 0 \le u \le 1-c \\ u-(1-c) & 1-c < u \le 1 \\ 0 & otherwise \end{cases} \tag{38}$$

where $c$ is a constant, $0 < c < 1$. Then, the

$$\min_{u\in[0,1]} \left|\Phi^{-1}(u) - \Phi^{-1}(g(u))\right| \tag{39}$$

will occur for a value of $u$ satisfying $\phi(x_u) = \phi(x_{g(u)})$.

Proof by contradiction: Assume that the

$$\min_{u\in[0,1]} |\Phi^{-1}(u) - \Phi^{-1}(g(u))| \tag{40}$$

will occur for a value of $u$ for which $\phi(x_u) \neq \phi(x_{g(u)})$. Let $u = u^*$ be such a value.

*Case 1.* $\phi(x_{u^*}) < \phi(x_{g(u^*)})$.

If $0 < u^* < 1-c$, then $u^* < g(u^*) \Rightarrow x_{u^*} < x_{g(u^*)}$. Choose an epsilon

$$0 < \epsilon < [\phi(x_{g(u^*)}) - \phi(x_{u^*})]/2. \tag{41}$$

Since $\phi(x)$ is continuous, we have by definition

$$|\phi(x_u) - \phi(x_{u^*})| < \epsilon \text{ whenever } |x_u - x_{u^*}| < \delta_1(\epsilon) \tag{42}$$

and

$$|\phi(x_u) - \phi(x_{g(u^*)})| < \epsilon \text{ whenever } |x_u - x_{g(u^*)}| < \delta_2(\epsilon). \tag{43}$$

Choose $\delta = \min(\delta_1, \delta_2)$. Within a $\delta$-neighborhood of $x_{u^*}$ and $x_{g(u^*)}$, the corresponding ordinates $\phi(x)$ do not overlap (reference Figure 5). Now, increment $u^*$ by an amount $\eta$; $u^* + \eta = u'$, such that $x_{u'} \in (x_{u^*} - \delta, x_{u^*} + \delta)$ and $x_{g(u')} \in (x_{g(u^*)} - \delta, x_{g(u^*)} + \delta)$. (Our choice of $\epsilon$ and $\delta$ guarantees that such an $\eta$-value exists.)

The relation

$$\int_{x_{u^*}}^{x_{u'}} \phi(x)dx = \eta = \int_{x_{g(u^*)}}^{x_{g(u')}} \phi(x)dx \tag{44}$$

must hold.

From the mean value theorem we have

$$(x_{u'} - x_{u^*})\phi(x') = (x_{g(u')} - x_{g(u^*)})\phi(x''), \tag{45}$$

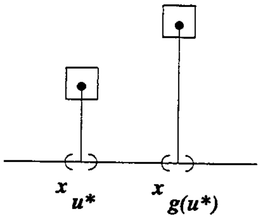

**Figure 5. Illustration of Case 1**

with

$$\phi(x') < \phi(x''). \tag{46}$$

This implies $x_{u'} - x_{u^*} > x_{g(u')} - x_{g(u^*)}$. Rearranging, $x_{g(u^*)} - x_{u^*} > x_{g(u')} - x_{u'}$. This means that $u^* \in (0, 1-c)$ cannot be optimal.

Consider now the complementary interval, $(1-c, 1)$.

If $1 - c < u^* < 1$, then $g(u^*) < u^* \Rightarrow x_{g(u^*)} < x_{u^*}$ and an appropriate graphic would be the mirror image of Figure 5.

The $\epsilon$, $\delta$, argument remains unchanged. Whereas before we considered an incremental value of $u^*$, we now consider a decremental value of $u^*; u^* - \eta = u'$, leading to

$$\int_{x_{g(u')}}^{x_{g(u^*)}} \phi(x)dx = \eta = \int_{x_{u'}}^{x_{u^*}} \phi(x)dx \tag{47}$$

and inequality $x_{g(u^*)} - x_{g(u')} < x_{u^*} - x_{u'}$. Rearranging, $x_{u'} - x_{g(u')} < x_{u^*} - x_{g(u^*)}$. This means that $u^* \in (1-c, 1)$ cannot be optimal. Case 1, $\phi(x_{u^*}) < \phi(x_{g(u^*)})$, cannot hold.

*Case 2.* $\phi(x_{u^*}) > \phi(x_{g(u^*)})$.

Reverting to case 1: $\phi(x_{u^*}) > \phi(x_{g(u^*)})$, and $u^*$ on the intervals $(0, 1-c)$, $(1-c, 1)$, an argument identical to that detailed above leads to the conclusion that $\phi(x_{u^*}) > \phi(x_{g(u^*)})$ cannot hold. The proof is thus established by contradiction. ■

Determination of

$$\min_{u \in [0,1]} |\Phi^{-1}(u) - \Phi^{-1}(g(u))| \tag{48}$$

is now straightforward; $\phi(x_u) = \phi(x_{g(u)})$ is satisfied when $u = 1 - g(u)$, with $g(u)$ as given in (38).

Solving for $u$, we obtain the values

$$u = \frac{1}{2}(1-c) \text{ and } u = 1 - \frac{c}{2} \tag{49}$$

for which $|\Phi^{-1}(u) - \Phi^{-1}(g(u))|$ must be evaluated to determine local extrema.

The minimum value may be expressed for $0 < c \leq \frac{1}{2}$ as

$$\min_{u \in [0,1]} |\Phi^{-1}(u) - \Phi^{-1}(g(u))| = 2\sigma z_{(1+c)/2}. \tag{50}$$

This value is monotone increasing over the specified interval. Over the entire interval, $0 < c < 1$, (50) is symmetric about $c = 1/2$, at which the global maximum is assumed. The entire function is graphed in Figure 6 for $\sigma = 1$.

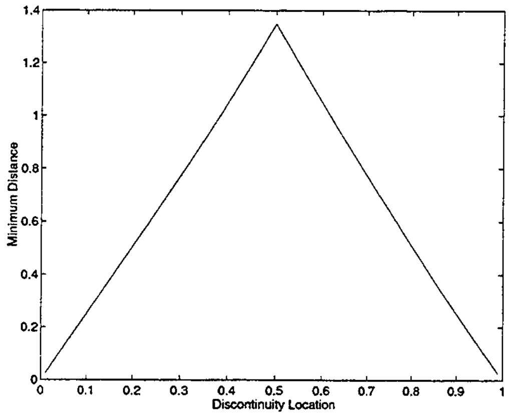

**Figure 6. Minimum Distance vs. Discontinuity Location**

# 5. Comparison of Noise Modulation Techniques

Both PLNM, presented in Section 4, and antipodal noise modulation, Section 3, modulate a binary input signal and produce Gaussian noise, regardless of the distribution of that input signal. We established that PLNM has greater noise immunity than the antipodal modulation by comparing the minimum Euclidean distance between modulation points, $d_{min}$, for each technique. Recall, in the presence of noise, a transmitted signal can be correctly detected if the distortion does not exceed a threshold value of $d_{min}/2$ [14]. For antipodal noise modulation this threshold is equal to 0, but for PLNM, $d_{min}/2 = 1.35\sigma/2$ and $\sigma^2$ can be adjusted to achieve the desired performance.

Traditionally, when detecting signals in the presence of AWGN, modulation techniques are compared by computing a probability of error, $P_e$. Let us assume a maximum *a posteriori* (MAP) detector with the binary information bits having equal probability of occurrence. Then, the probability of error can be computed using the distance between the modulation points and the power of the channel AWGN.

We begin with the familiar case of uncoded antipodal (binary) modulation and use a traditional modulation technique by which to compare our two noise modulation methods. For all methods, let us denote a modulated signal as $s$ and the channel AWGN as the signal $v$ with power $\sigma_v^2$. Then, the probability of error for uncoded antipodal modulation with modulation values of $s = m \in \{\pm 1\}$ is

$$P_e = \mathrm{Q}\left(\frac{A}{\sqrt{2N_o}}\right) = \mathrm{Q}\left(\frac{2}{2\sigma_v}\right), \tag{51}$$

where Q represents the complementary error function, $A$ is equal to the distance between the modulation signals, $|s(m_i = -1) - s(m_i = 1)|$, and $\sigma_v^2 = N_o/2$ [14].

The noise modulation techniques considered in this paper produce Gaussian noise. Therefore, the probability of error is conditional upon the value of a random variable. Consequently, the conditional probability of error for the antipodal noise modulation can be expressed as

$$P_{e|n} = \mathrm{Q}\left(\frac{2|n|}{2\sigma_v^2}\right) = \mathrm{Q}\left(\frac{|n|}{\sigma_v^2}\right), \tag{52}$$

with $n \sim N(0, \sigma_n^2)$. For PLNM, the conditional probability of error is

$$P_{e|u} = \mathrm{Q}\left(\frac{\sigma_n|\Phi^{-1}(u) - \Phi^{-1}(g(u))|}{2\sigma_v}\right), \tag{53}$$

where $u \sim U(0,1)$.

To present the probability of error for antipodal noise modulation and PLNM as a function of the signal-to-noise ratio (SNR), we compute the expected probability of error by weighting the conditional probability of error with the probability distribution of the random variables $n$ and $u$, respectively.

The two noise modulation techniques are compared in Figure 7, where the expected $P_e$ in relation to SNR is shown. In addition, the $P_e$-SNR performance of uncoded antipodal modulation has been included to demonstrate the relation of noise modulation to uncoded modulation.

As is demonstrated in Figure 7, the antipodal noise modulation experiences a floor effect with the expected $P_e$ not less than $10^{-2}$ at 30 dB SNR. The PLNM has much better performance than the antipodal noise modulation and is similar to that of uncoded binary modulation. Of course, the uncoded antipodal modulation has better $P_e$ performance than PLNM because the uncoded signal is not constrained to follow a Gaussian distribution (hidden in noise). The performance difference between uncoded modulation and PLNM can be attributed to hiding the transmitted data in a Gaussian noise. This hiding exhibits a 2.36 dB loss in SNR at a $P_e$ equal to $10^{-10}$.

# 6. Conclusions

In this paper, we presented a modulation technique to embed a binary bitstream within a real-valued Gaussian noise sequence that possesses a minimum distance property to promote accurate detection. The resultant signal is Gaussian in nature and is difficult to intercept due to its low power. The technique can be used to hide information within a noise sequence that is then added to a carrier for a variety of applications. In addition, we established that the PLNM modulation function is an optimal mapping that maximizes the minimum distance between modulation points while meeting the desired stochastic constraint.

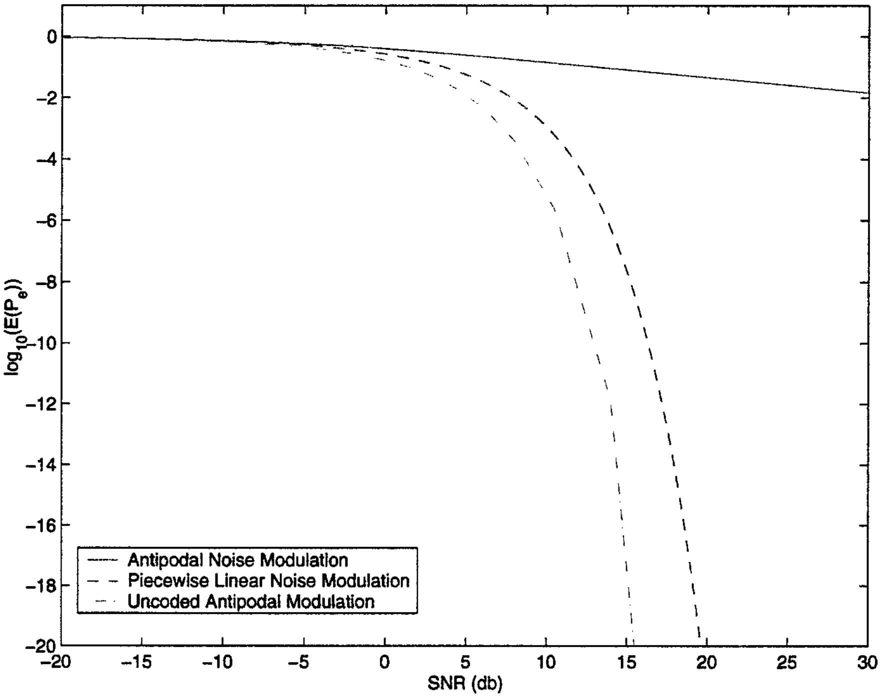

**Figure 7. Comparison of Modulation Techniques**

There are some extensions of this work that were deemed to be beyond the scope of this paper. The effect of more than one discontinuity on the value of $d_{min}$ in the PLNM procedure was not investigated. Additionally, it may be possible to follow the PLNM framework established here to embed information within non-Gaussain noise sequences that hold importance in application.

INTENTIONALLY LEFT BLANK.

# 7. References

[1] Smith, J. R. and B. O. Comisky. "Modulation and Information Hiding in Images." In R. Anderson, editor, *Information Hiding, First International Workshop*, vol. 1174 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, pp. 207–226, 1996.

[2] Marvel, L. M., C. G. Boncelet, Jr., and C. T. Retter. "Spread Spectrum Image Steganography." *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075–1083, August 1999.

[3] Hartung, F. and B. Girod. "Fast Public-Key Watermarking of Compressed Video." In *Proceedings of the IEEE International Conference on Image Processing.* Santa Barbara, CA, October 1997.

[4] Shannon, C. E. "Communication in the Presence of Noise." *Proceedings of the Institute of Radio Engineers*, vol. 37, pp. 10–21, 1949.

[5] Viterbi, A. J. "Wireless Digital Communications: A View Based on Three Lessons Learned." *IEEE Communications Magazine*, vol. 29, no. 9, pp. 33–36, September 1991.

[6] Scholtz, R. A. "The Spread Spectrum Concept." *IEEE Transactions on Communications*, vol. 25, no. 8, pp. 748–755, August 1977.

[7] Simon, M. K., J. K. Omura, R. A. Scholtz, and B. K. Levitt. *Spread Sprectrum Communications, Volume I.* Computer Science Press, Rockville, MD, 1985.

[8] Wilks, S. S. *Mathematical Statistics.* John Wiley and Sons, Inc., New York, NY, 1962.

[9] Abramowitz, M. and I. A. Stegun. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables.* Dover Publicatons, Inc., New York, NY, 1964.

[10] Hoel, P. G. *Introduction to Mathematical Statistics, 2nd Ed..* John Wiley and Sons, Inc., New York, NY, 1960.

[11] Walpole, R. E., R. H. Myers, and S. L. Myers. *Probability and statistics for engineers and scientists, 6th Ed..* Prentice-Hall, Upper Saddle River, NJ, 1998.

[12] Ross, S. *A First Course in Probability, 3rd Edition.* Macmillan Publishing Co., New York, NY, 1988.

[13] Olmsted, J. M. H. *Advanced Calculus.* Appleton-Century-Crofts, Inc., New York, NY, 1961.

[14] Sklar, B. *Ditial Communications: Fundamental and Applications.* Prentice-Hall, Inc., Englewood Cliffs, NJ, 1988.

INTENTIONALLY LEFT BLANK.

NO. OF COPIES ORGANIZATION

2 DEFENSE TECHNICAL
INFORMATION CENTER
DTIC DDA
8725 JOHN J KINGMAN RD
STE 0944
FT BELVOIR VA 22060-6218

1 HQDA
DAMO FDT
400 ARMY PENTAGON
WASHINGTON DC 20310-0460

1 OSD
OUSD(A&T)/ODDDR&E(R)
R J TREW
THE PENTAGON
WASHINGTON DC 20301-7100

1 DPTY CG FOR RDA
US ARMY MATERIEL CMD
AMCRDA
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001

1 INST FOR ADVNCD TCHNLGY
THE UNIV OF TEXAS AT AUSTIN
PO BOX 202797
AUSTIN TX 78720-2797

1 DARPA
B KASPAR
3701 N FAIRFAX DR
ARLINGTON VA 22203-1714

1 US MILITARY ACADEMY
MATH SCI CTR OF EXCELLENCE
MADN MATH
MAJ HUBER
THAYER HALL
WEST POINT NY 10996-1786

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL D
D R SMITH
2800 POWDER MILL RD
ADELPHI MD 20783-1197

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL DD
2800 POWDER MILL RD
ADELPHI MD 20783-1197

NO. OF COPIES ORGANIZATION

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CI AI R
RECORDS MGMT
2800 POWDER MILL RD
ADELPHI MD 20783-1145

3 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CI LL
2800 POWDER MILL RD
ADELPHI MD 20783-1145

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CI AP
2800 POWDER MILL RD
ADELPHI MD 20783-1197

ABERDEEN PROVING GROUND

4 DIR USARL
AMSRL CI LP (BLDG 305)

NO. OF
COPIES ORGANIZATION

2 COMMANDER
US ARMY CECOM RDEC
AMSEL RD ST SP P VAN SYCKLE
FT MONMOUTH NJ 07703

1 COMMANDER
US ARMY CECOM RDEC
AMSEL RD IW DE B PEARLMAN
FT MONMOUTH NJ 07703

2 UNIVERSITY OF DELAWARE
DEPARTMENT OF ELECTRICAL ENG
C BONCELET JR
NEWARK DE 19716

ABERDEEN PROVING GROUND

22 DIR USARL
AMSRL RO T
DR W Sander
AMSRL CI
DR N RADHAKRISHNAN
DR J GANTT
AMSRL CI C
DR J GOWENS
AMSRL CI CT
F BRUNDICK
G HARTWIG
AMSRL CI CN
G. RACINE
DR L MARVEL (15 copies)

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project(0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
April 2001

3. REPORT TYPE AND DATES COVERED
Final, August 1998 - November 2000

4. TITLE AND SUBTITLE
Piecewise Linear Noise Modulation (PLNM)

5. FUNDING NUMBERS
P611102AH48

6. AUTHOR(S)
Lisa M. Marvel, Malcolm S. Taylor, and Charles G. Boncelet, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRL-CI-CT
Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-2450

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

10.SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT*(Maximum 200 words)*

We present a modulation technique to embed a binary bitstream within a real-valued Gaussian noise sequence. The modulation produces a sequence which possesses an optimal minimum distance property that promotes accurate detection when the sequence has been exposed to noise. Because the modulated sequence possesses Gaussian properties and has low power, it is difficult for unintended parties to intercept and detect the signal. The technique can be used to hide information in a signal that is then added to a carrier for a variety of applications.

14. SUBJECT TERMS
noise modulation, steganography

15. NUMBER OF PAGES
23

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UL

INTENTIONALLY LEFT BLANK.

## USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-TR-2450 (Marvel) Date of Report April 2001

2. Date Report Received ______

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) ______

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) ______

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. ______

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) ______

CURRENT ADDRESS

Organization

Name E-mail Name

Street or P.O. Box No.

City, State, Zip Code

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS

Organization

Name

Street or P.O. Box No.

City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)

**(DO NOT STAPLE)**

DEPARTMENT OF THE ARMY

OFFICIAL BUSINESS

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

**BUSINESS REPLY MAIL**
FIRST CLASS PERMIT NO 0001, APG, MD

POSTAGE WILL BE PAID BY ADDRESSEE

DIRECTOR
U.S. ARMY RESEARCH LABORATORY
ATTN AMSRL CI CT
ABERDEEN PROVING GROUND MD 21005-5067